PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel Security Breach Notification and Mitigation Services Records
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒	**New DoD Information System**	☐	**New Electronic Collection**
☐	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	Pending
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☐ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 20

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. 10/16/2015

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number	3206-0032
Enter Expiration Date	March 31, 2017

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The E-Government Act of 2002 (Pub. L. No. 107-347); the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283) (44 U.S.C. 3551-3559); 10 U.S.C. 113, Secretary of Defense; 50 U.S. C. 3038, Responsibilities of Secretary of Defense Pertaining to National Intelligence Program; E.O. 12333, United States Intelligence Activities, as amended; E.O. 13402, Strengthening Federal Efforts to Protect Against Identity Theft, as amended; E.O. 13526, Classified National Security Information; White House Memorandum dated September 20, 2006, Subject: Recommendations for Identity Theft Related Data Breach Notification; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To provide breach notification and facilitate the provision of breach mitigation services to individuals affected by the breach of information in the Office of Personnel Management (OPM) background investigation databases. DoD will also use the data to respond to breach verification inquiries received from individuals using the link on OPM's website that redirects individuals to a DoD website where they can enter their information to find out if they have been affected by this breach. These records may also be used for tracking, reporting, measuring, and improving the Department's effectiveness in implementing this data breach notification.
Types of personal information being collected are last, first, and middle name, Social Security Number (SSN), date of birth, place of birth, citizenship status, country of citizenship, home and/or business addresses, phone numbers, and e-mail addresses.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Risk includes unauthorized access to individual's PII. Access to PII is restricted to those who have a need-to-know in the performance of their official duties in connection with the breach notification process. Access to PII is further restricted by the use of Personal Identity Verification (PIV) cards and PIN. Physical entry is restricted by the use of locks, key cards, security guards, and identification badges. All individuals granted access to this system of records will have completed annual Information Assurance and Privacy Act training and be appropriately vetted. Audit logs will be maintained to document access to data. All electronic data transfers into this system of records will be encrypted. Records will be maintained in a secure database with an intrusion detection system in a physically controlled area accessible only to authorized personnel.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** ~~(Enter name and describe the language in the contract that safeguards PII.)~~

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Commercial entities under contract with DoD for the sole purpose of verifying

addresses of affected individuals for notification purposes.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individual's are informed that providing the information is voluntary. This voluntary disclosure is given on the SF-85, 85P, Questionnaire for Position of Public Trust; SF-86, Questionnaire for National Security Position; as well as the website where individuals can enter their information to find out if they have been affected by this breach.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Yes. By signing and/or submitting the SF-85, SF-85P, SF-86 or information to the website, individuals are consenting to the specific uses identified in the Privacy Act Statement and System of Records Notice.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

AUTHORITY: The E-Government Act of 2002 (Pub. L. No. 107-347); the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283) (44 U.S.C. 3551-3559); 10 U.S.C. 113, Secretary of Defense; 50 U.S.C. 3038, Responsibilities of Secretary of Defense Pertaining to National Intelligence Program; E.O. 12333, United States Intelligence Activities, as amended; E.O. 13402, Strengthening Federal Efforts to Protect Against Identity Theft, as amended; E.O. 13526, Classified National Security Information; White House Memorandum dated September 20, 2006, Subject: Recommendations for Identity Theft Related Data Breach Notification; and E.O. 9397 (SSN), as amended.

PURPOSE: To provide breach notification and facilitate the provision of breach mitigation services to individuals affected by the breach of information in the Office of Personnel Management (OPM) background investigation databases. DoD will also use the information to respond to breach verification inquiries received from individuals using this DoD website. These records may be used for tracking, reporting, measuring and improving the Department's effectiveness in implementing this data breach notification.

ROUTINE USE: In addition to disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD to commercial entities for address verification purposes. Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, Disclosure to the Office of Personnel Management Routine Use, Counterintelligence Purpose Routine Use and Data Breach Remediation Purposes Routine Use. The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

DISCLOSURE: Voluntary. However, failure to provide requested information may prevent or delay DoD's ability to verify and/or notify an individual affected by the breach of information in the OPM background investigation database.
This Privacy Act Statement is currently under legal review

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.